Copy sent DD(CSA) 15(I)

TOP SECRET "U" 1. TICOM/I-92

FINAL INTERROGATION OF

WACHTMEISTER OTTO BUGGISCH (OKH/IN. 7/VI AND OKW/CHI).

Attached is a report on the final interrogation of BUGGISCH carried out by Major Bundy at Oberursel on 25th August, 1945.

The report supplements and concludes the notes in TICOM/I-58 and I-64, and also covers questions raised by BUGGISCH's written work.

TICOM
11 Sept. 1945

Copy No. 20
No. of Pages 6

DISTRIBUTION

British

1. Director
2. D.D.3
3. D.D.4
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt. Col. Leathem
10. Major Morgan

U.S.

11-12. OP 20-G (2) (via Lt. Pendergrass)
13. G-2 (via Lt. Col. Hilles)
14-15. S.S.A. (2) (via Major Seaman)
16. Director, S.I.D. USFET (via Lt. Col. Johnson)
17. Col. Lewis Powell

TICOM

18. Chairman
19-20. C.A.C. (2)
21. Cdr. Bacon
22. Cdr. Mackenzie
23. Cdr. Tandy
24. Lt. Col. Johnson
25. Lt. Cdr. Manson
26. Major Seaman
27. Lt. Vance
28. Capt. Cowan
29. Lt. Fehl
30-31. Ticom Files (2)

Additional

32. Mr. Twinn
33. Lt. Col. Pritchard

FINAL INTERROGATION OF

WACHTMEISTER OTTO BUGGISCH (IN 7/VI AND OKW/CHI)

AT OBERURSEL, 25 AUGUST 1945

1. M40. (See I-58. This was a machine designed by MENZER in 1940 and never put into use).

This was mechanical in operation. It was a cylinder, with about 30 slots for cipher alphabets. These slots were rotated by a hand crank, and might move from 0 to 3 slots after each letter. The plain text alphabet was mixed and was in a fixed horizontal slot. The plain text was enciphered by reading from this plain text alphabet to the cipher alphabet which had been brought next to it. Buggisch described the principle as that of the "TRITTHEIM" TABLE, a historic cryptographic principle from the 17th Century (= U.S. "polyalphabetic").

The motion was governed by 3 (or possibly 4) wheels with positive and negative lug settings as with the Hagelin machine. The motion was the sum of the positive settings, subject to an overlap principle as with M 209. Buggisch did not know the cycle of the motion wheels or the details of the construction by which they acted to vary the motion when the crank was turned.

Additional security was provided by using only 36 strips at one time, leaving about 4 slots blank. When these slots reached the enciphering position a random letter was chosen and inserted in the cipher text, and the plain text letter was enciphered by the next strip that came to the enciphering position.

No ideas were ever formulated on the total number of strips to be used, or the frequency of setting changes. Preliminary tests by LOERING and BUGGISCH gave the machine a high security rating. However it was just as bulky as the ENIGMA and could not print letters, which was then the chief improvement desired. For these reasons it was rejected, and only a lab model was ever built.

2. Solution of Croat Enigma. This was not an outstanding cryptanalytic achievement. The machine used was the K model, with three wheels and no stecker. The machines were made for the Croats by the firm of KRONSKY and KRUGER, Berlin, which gave the wirings promptly to OKW/WNV in about 1941 or 1942. A single key was used throughout the entire Croat Army and area, and this consisted only of a list of 100 settings for a period of a month. As far as Buggisch knew the Ringstellung stayed always at AAA, and the wheel order at 1, 2, 3. Just to make sure, the Germans paid for one of the first keys used, and with this decoded traffic were able to establish stereotypes and solve almost 100% from the first.

The solutions were done entirely by hand with wiring charts, assuming a pet beginning (one third of all messages began with "MINORS") and assuming the left hand wheels and Umkehrwalz unmoving (only one notch per wheel as in the commercial model). The Croats also had pet indicators and so would furnish depths in case this method did not work. The setting was indicated directly by a two digit number unenciphered, so that the settings were solved almost as fast as they came, and the traffic read currently from then on. Buggisch did not recall the contents in detail. 90% of it was uninteresting; there were some interesting messages about actions against TITO.

Buggisch said the Germans had considered equipping the Croats with the military Enigma, as they did for HUNGARY, ROUMANIA, FINLAND, and ITALY (and JAPAN, he thinks) in about 1942. However, they decided against this as they believed the corrupt CROATS would go right on selling the keys to British agents, while they, the GERMANS, would have to pay as well instead of solving free. (The possibility of a BRITISH solution obviously did not occur to Buggisch during this discussion of the K model.)

3. Complications in C36. Buggisch could recall no "complicated enciphering device," unless he had meant to refer to the new indicator method introduced in January of 1944. The old indicator system, changed in its details in 1942, had been a letter substitution table, which had been simple. The new system was based on numbers, but he could give no details. Relative internal settings continued to be recovered and a high percent of the traffic solved on cribs and statistics (for any message over 400 letters) until the indicator system was broken in the late summer of 1944.

About the same time in 1944 the French had adopted a system of sending internal settings by means of an ordinary sentence for each wheel, of which the first so many nonrepeating letters gave the active lug positions. This system was first reported in a broken code message; the knowledge that it existed was of academic interest only, as no keys were gained from other systems.

Buggisch spoke especially of the successful solution of C36 in 1943, on de GAULLE traffic to CORSICA. He also said that the Southern France landings were largely given away as to date and strength of force by broken C36 traffic.

4. "W-Square" -- After some pondering Buggisch finally came to the obvious solution that it was a mistaken reading for Omega Square. This was a well-known statistical test used in probability calculations. It had been invented by GEBELEIN, a German mathematician, who had published a full description of it in the "Zeitschrift fuer Angewandte Mathematik" shortly before the war. The test was a great favorite of v. DENFFER of OKH, who preferred it to the alternative CHI test of the American Mathematician, PIERSON.

Von DENFFER (and Buggisch on occasion) had used the test in preliminary analysis of any traffic thought to be machine, or indeed for any unknown traffic including codes. In the beginning of 1944 he had used it on C36 traffic in an effort to find out if the old internal setting period (10 days, Buggisch thought) had been altered along with the indicator system. He thought that he could establish a change of internal setting by letter count; in fact the results had been inconclusive, and the new period established by actual solutions more rapidly.

5. Conversations with KorvettenKapitaen JAECKLE. Buggisch considered this a very foolish incident altogether. He had become acquainted with JAECKLE in 1943 very briefly. JAECKLE was an ordinary Naval Signals Officer, who had got hold of a model of the M209 and had worked out a "solution" while sitting idle in a French port. The solution was in fact childish and consisted of nothing more than a study of the theoretical working equation of the machine. JAECKLE had talked his way to SKL and had talked a lot about getting a section of 200 men to work on the machine. Actually he had been exposed quickly and sent back to sea after three or four months. Buggisch had seen nothing of him since.

6. Russian Systems. K37 and OK 40 were Russian names established from captured material. The successor to OK40 was called K1, he believed.

7. Typex and Enigma Documents. The documents left in the MATTHEIKIRCHPLATZ were only reports on mathematical studies, photostats of reports already referred to in Buggisch's write-up, and photostats of the British documents captured at DUNKIRK.

8. American Strip Traffic. Buggisch does not know what links were broken in 1942, but he thinks they were chiefly diplomatic, and recalls the mention of CAIRO in particular.

9. OKW Analytic Machinery was last seen in the cellar of the HAUS DES FREMDEN VERKEHRS on the 24th of January, 1945. Buggisch thought it was to go to HALLE with HUETTENHAIN.

10. K37 differed from B211 in lacking the "Surchiffreur", or "Ueberschluesseler", a sort of Enigma wheel by which the path of the current was turned to another channel at one point, crossing over and exchanging positions with another path instead of continuing parallel. Buggisch called this an X effect, and said it greatly complicated analysis, as it was hard to tell when it was being employed in place of the parallels.

11. Security Conferences with General GIMMLER. These took place over a period of three months from November 1944 through January 1945. GIMMLER insisted on them, though HUETTENHAIN felt it was a waste of time simply to gather formally to hear reports. In spite of this feeling HUETTENHAIN was in the chair at the sessions. Four different subjects were covered, with a day allotted to each. These were: a) Speech Encipherment b) Security of Teletype Cipher Machines c) Security of ENIGMA d) Security of Hand Systems. Buggisch himself attended only the sessions on Speech Encipherment and on ENIGMA. However, he had a hearsay account of the other sessions from PIETSCH and DOERING, who attended all.

a). Speech Encipherment. 24 Jan. 1945. This was a most inconclusive session, and hardly any discussion was aroused. Papers were read by METTIG on the use of cover names for protecting ordinary phone conversations, by LIEBKNECHT on the technical aspects of speech-scrambling devices, by Buggisch (after lunch, alas!) on the mathematical analysis of speech scrambling, and by LOTZE (of Gruppe IV, WAPRUEF 7) on the technical aspects of devices for reading scrambled speech. B. said the whole affair was a farce and a waste of time, and led to no closer liaison between the would-be makers and breakers.

b) Teletype Cipher Machines. The replacement of T52c by T52d and -e had been discussed and approved. The SZ42 was still thought to be better but the possibility was discussed of giving it an irregular and interacting motion and also a daily stecker - like monoalphabetic change superimposed. DOERING was working along these lines with Uffz. LINDMEIER.

c) ENIGMA. There were two sessions on ENIGMA, one of which was devoted largely to the Naval machine. The Naval session was attended by Kapitän SINGER and another OKM officer. Hptm. PORT, the head of the OKL security section, participated along with Reg.Rat Prof. HOHEISEL (who had entered the OKL only in 1944 but was already rated the brains in an otherwise weak section).

The conference confirmed the decision, already effective in practice, to drop the "K" and "G" (Abwehr) models of the ENIGMA, except that the railways could go on using the "K" for routine messages of

no security content. Messages of any security content were to be enciphered twice by the "K" machine (but Buggisch does not know whether this was ever done in fact). The "G" machine was already dropped everywhere, having been replaced on a few military attaché nets by the military model.

Worry was also expressed over the fact that the military machine had not been changed throughout the war. Varying solutions were discussed, Buggisch himself approving of the OKL device of Enigma UHR. The idea of LÜCKENFÜLLERWALZE was also approved.

d) Hand Systems. There were no significant results at the conference on this subject. It was agreed by all that NS 42 and TS 42 (double and single "Playfair") were insecure, and the introduction of RASTER was approved.

In general, the meetings were exchanges of information rather than being bound to come to a decision.

12. "FALL WICHER" (Polish Solution of Enigma.) This was the name given to the definite proof received in 1943 or 1944 that the Poles had read Enigma up to the outbreak of war and for some time after, in POLAND and later in FRANCE. Buggisch thought that "WICHER" was the Polish cover name for the solution operation.

Buggisch began by relating an interesting prelude. In 1939 and early 1940 IN 7/IV (as it was then), specifically PIETSCH, STEINBERG, and one BOHM (who was later released from the office for reasons unknown) had done theoretical work and had come to the conclusion that the doubled encipherment of indicators was not secure. There were, moreover, a few scattered bits of evidence found in the Polish cipher office at WARSAW that the Poles had possessed a section of extraordinary security. Enigma solution, however, was pooh-poohed. As a result of the theoretical work alone, IN 7/IV was able to force a change in the indicator system early in 1940.

Very much later, in 1943 or 1944, two Polish officers, a Lt. Col. and a Major, made some disclosures at a German PW Camp in HAMBURG. As a result PIETSCH was sent to interrogate them, and PIETSCH later told Buggisch about their general story, without the details unfortunately. It boiled down to a clear claim that the Poles had read ENIGMA for several years before the war (Buggisch thought that it was very bad usage, giving depths, which caused most of this, rather than the indicator system). After the short Polish campaign the Poles had moved to FRANCE and had probably worked on it there. Solution had stopped, however, and Buggisch could say only that it was an abrupt ending, as if caused by a change in the system. This he naturally assumed (as presumably did PIETSCH) was the change in the indicator system.

PIETSCH told Buggisch that he did not bother to get the details of the Polish method. Buggisch himself reiterated his belief that it could have been done with a large Hollerith machine complex as one method, but he had never heard any suggestion that the Poles had such an apparatus. Buggisch also recalled that the officers said that the leading workers were two very young men, math students, and this was linked with the capture of two such men in WARSAW in 1939. They were not traced so far as he knew. Buggisch did not know their names, but thought PIETSCH would.

13. OKH/Chi Organization. Buggisch was unable to add any new names or to throw new light on the organization and membership of the linguistic sections as given by HERZFELD. He gave a detailed account of the growth and development of the Mathematical Referat.

The origins of the math Referat were in the old IN 7/IV in 1939-1940. It was then concerned with security of German systems only (witness the job on ENIGMA) and had about a dozen mathematicians including PIETSCH, STEINBERG, BÖHM (see supra, later released), v. DENFFER, HILBURG, and LUZIUS. Most of these were drawn from the statistical offices of insurance companies. Buggisch had his first contact with this group at the end of 1940 as a result of his work on the C36.

IN 7/VI was set up at the beginning of 1941, and a math referat created. The grouping was loose at first, as men would be detached for specific projects in security work or in some national referat. The work gradually divided itself into three parts, general theory (Referat F, under v. DENFFER), hand systems (Referat 7?, under Oblt. LÜDERS), and machine systems (Referat 13 under Wachtmeister DOERING). Buggisch himself was deputy to DOERING.

At the end of 1942 (later according to HERZFELD, but the outline is the same) all the varied Referats were grouped into two Hauptreferats, "A", for languages, under BAILOVIC, and "B", for math studies, under PIETSCH. The latter comprised the three former Referats, F, 7, and 13. This organization remained in effect as long as Buggisch was there. (For later organization see HENTZE and HARRENBERG accounts.)

V. DENFFER's Referat included HILBURG, RINOW, and WÜNSCHE as its best men. Under LÜDERS were his deputy, uffz. JESSE, and FRIEDE, FÖPPL, and WACHTMEISTER DREESEN (helper only). DOERING's section had Buggisch himself and Wachtmeister VALENTIN, who succeeded him as deputy, and Uffze. MUELLER, DIEHL, and SAUER and Gefr. JAUSEL (helpers only). The section also had various men with particular specialities, LINDMEIER and LACHNER on teletype security (note that LACHNER is elsewhere noted by KARRENBERG as the specialist in American traffic) and TROEBUCHER on Russian systems including BAUDOT (Troebucher spent most of his time with LNA).

The above are not all the names that Buggisch could have recalled in time, he said, but they include the foremost technicians of all sections.